AuthPoint

L'authentification multifacteur (MFA) ? Un jeu d'enfant !

L'utilisation d'identifiants volés afin de réaliser une intrusion est la tactique la plus souvent utilisée par les pirates informatiques.* En demandant des preuves d'identité supplémentaires qui vont au-delà du simple mot de passe, l'authentification multifacteur est l'unique dispositif de sécurité capable de protéger votre entreprise.

La solution d'authentification multifacteur (MFA) unique de WatchGuard permet non seulement de réduire les risques d'intrusion sur le réseau et de fuites de données en cas d'identifiants perdus ou vulnérables, mais est en plus hébergé dans le Cloud, pour une configuration simple et une gestion en continu. En outre, AuthPoint ne se contente pas de la traditionnelle authentification à 2 facteurs (2FA), puisqu'il propose des modes d'identification des utilisateurs innovants tels que notre option ADN de l'appareil mobile. Grâce à notre vaste écosystème d'intégrations tierces, nous pouvons déployer une solide protection sur votre réseau, vos VPN, vos applications Cloud – partout où c'est nécessaire. Même les utilisateurs non spécialistes trouvent l'application mobile AuthPoint facile d'utilisation. Bref, WatchGuard AuthPoint™ est la solution idéale pour implémenter l'authentification multifacteur dans les entreprises qui cherchent à bloquer ce type de risques.

Protection MFA efficace grâce à l'ADN de l'appareil mobile.

L'authentification multifacteur demande aux utilisateurs de fournir des informations qu'ils connaissent (nom d'utilisateur et mot de passe), des informations sur quelque chose qu'ils possèdent ainsi que d'autres facteurs spécifiques à la personne. AuthPoint fournit un produit MFA hautement sécurisé à l'aide d'un message push, d'un QR code et d'un mot de passe à usage unique (OTP) ; notre ADN de l'appareil mobile établit une correspondance avec le téléphone de l'utilisateur lorsqu'il souhaite accéder à des systèmes ou applications. Ainsi, le pirate informatique qui clone l'appareil d'un utilisateur afin d'accéder à un système protégé est immédiatement bloqué, car l'ADN de l'appareil est différent.

Application mobile AuthPoint simple d'utilisation

L'application AuthPoint de WatchGuard permet aux utilisateurs de s'identifier directement depuis leur téléphone ! Inutile de porter un porte-clés ou une clé USB ; il vous suffit d'installer et d'activer l'application AuthPoint en quelques secondes pour vous identifier directement depuis un smartphone. Elle permet de procéder à une authentification push rapide ainsi qu'à une authentification hors ligne à l'aide de QR code et de l'appareil photo du téléphone. L'application est disponible en 11 langues et peut être téléchargée gratuitement dans l'AppStore et Google Play.

Couverture étendue avec le Web SSO

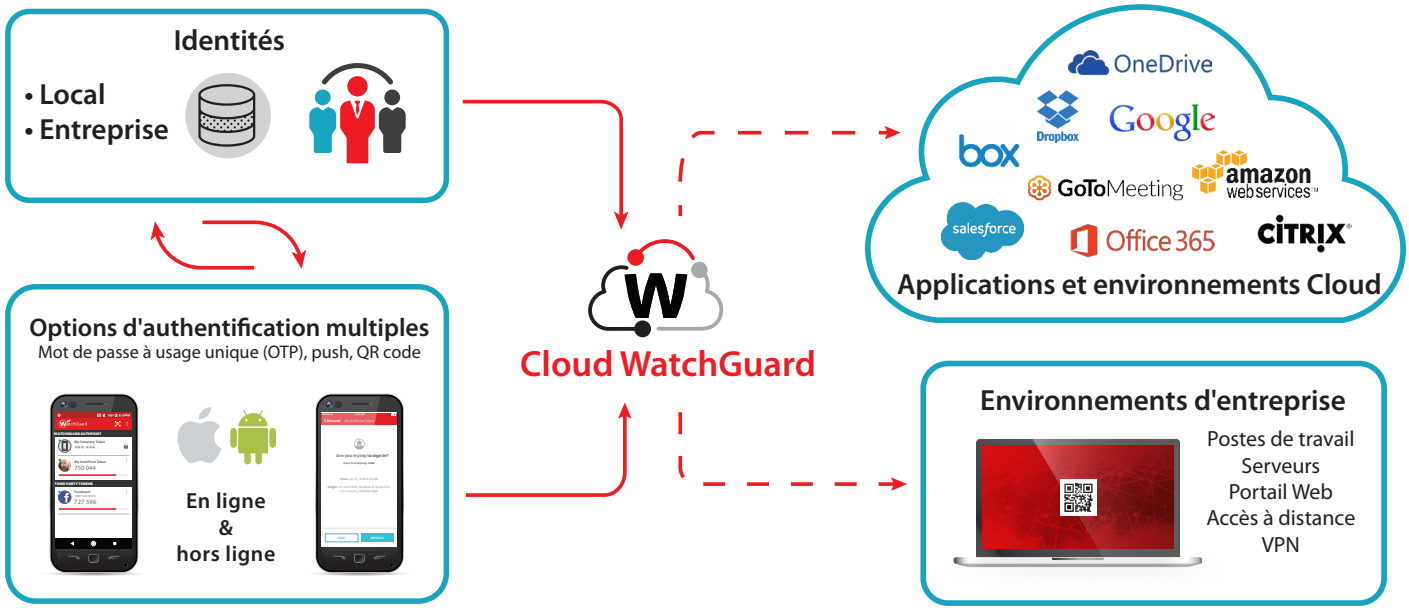
L'écosystème de WatchGuard inclut des dizaines d'intégrations tierces avec AuthPoint – il permet aux entreprises de demander aux utilisateurs de s'identifier avant d'accéder à des applications, VPN et réseaux sensibles sur le Cloud. AuthPoint prend en charge la norme SAML, qui permet aux utilisateurs de s'authentifier une fois afin d'accéder à toute une série d'applications et de services. En outre, l'identification sécurisée garantit une authentification en ligne et hors ligne aux ordinateurs Windows et Mac qui utilisent l'application AuthPoint.

Service Cloud avec un faible coût total de possession

Les entreprises qui possèdent un personnel informatique et une expertise en sécurité limités auront les avantages de la protection MFA, qui est facile à déployer et à gérer depuis le Cloud. AuthPoint fonctionne sur la plateforme Cloud de WatchGuard et est disponible quel que soit votre emplacement. Il n'est pas nécessaire d'installer un logiciel, de procéder à des mises à niveau ou de gérer des correctifs. Par ailleurs, la plateforme prend en charge aussi bien un compte global unique que de nombreux comptes indépendants ; les entreprises multisites et les fournisseurs de services managés peuvent donc afficher uniquement les données pertinentes pour la fonction d'une personne.

**Verizon, « 2018 Data Breach Investigations Report » (Rapport 2018 sur les atteintes à la sécurité des données)*

Éloigner les imposteurs des réseaux, VPN, ressources sur le Cloud et bien plus !



Plateforme Cloud de WatchGuard

- Gestion à 100 % sur le Cloud
- Attribution et activation d'un authentificateur
- Stratégies d'authentification basées sur les groupes et les ressources
- Journaux et rapports
- Accès basés sur les rôles
- Interface utilisateur intuitive et attrayante

Application mobile AuthPoint

- Trois méthodes d'authentification:
  1. Push
  2. Mots de passe à usage unique (OTP)
  3. QR code pour une utilisation hors ligne
- Authentificateur mobile – inutile de porter du matériel supplémentaire
- 11 langues
- Prise en charge de jetons multiples
- iOS and Android – téléchargement gratuit
- Protection PIN/biométrique (sur certains téléphones)
- ADN de l'appareil mobile – facteur d'authentification ajouté
- Transfert libre des jetons mobiles sur de nouveaux téléphones

Passerelle AuthPoint

- Passerelle de réseau d'entreprise
- Authentification et synchronisation des utilisateurs AD et LDAP
- RADIUS proxy

Agents AuthPoint

- Intégration dans des applications tierces sans support MFA natif
- Protection de l'identification sur ordinateur pour Windows et macOS

Écosystème AuthPoint

- Intégration de la MFA aux ressources, applications, bases de données et ressource du Cloud
- Prise en charge des normes SAML et RADIUS
- Guides d'intégration complets pour de nombreuses solutions tierces

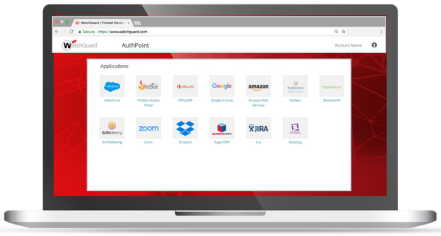
Cas d'utilisation recommandés

VPN / Accès à distance

Même expérience utilisateur que « identifiant + mot de passe »,

MAIS plus sécurisé et confirmation en un seul clic.

1. Demande de connexion avec nom d'utilisateur et mot de passe
2. Confirmation de la connexion VPN – demande sur l'application AuthPoint



Applications Cloud – Web SSO

1. Accéder au Portail d'Identité (IdP)
2. S'authentifier à l'aide d'un mot de passe à usage unique (OTP), d'un push ou d'un QR code
3. Accès à toutes les applications qui vous sont autorisées – inutile de s'authentifier une nouvelle fois !

Identification sur PC – Authentification en ligne

1. Cliquez sur « Envoyer une push »
2. Confirmez la demande d'identification du PC avec l'application AuthPoint
3. Vous êtes authentifié

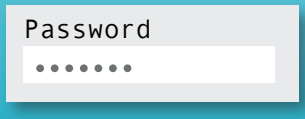
Identification sur PC – Authentification hors ligne

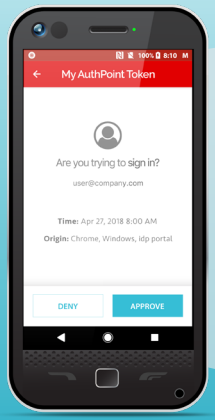
1. Sélectionnez « QR code » pour vous authentifier
2. Scannez le QR code à l'aide de l'application AuthPoint
3. Dans cet exemple, vous devez saisir la réponse 717960

Qu'est-ce que l'authentification multifacteur (MFA) ?

Il s'agit de l'utilisation de 2 facteurs d'authentification ou plus basés sur :

- **Quelque chose que vous connaissez**
  (mot de passe, code PIN)
- **Quelque chose que vous possédez**
  (jeton, téléphone portable)
- **Un attribut physique**
  (empreinte digitale, visage)





Facteurs AuthPoint :

1. **Votre mot de passe**
2. **Approbation sur votre authentificateur mobile**
3. **ADN du téléphone mobile correct**
4. **Une empreinte digitale pour bénéficier de l'accès**
   (sur certains modèles de téléphones)

AuthPoint respecte sa promesse d'authentification multifacteur en limitant le risque d'entreprise inhérent aux mots de passe vulnérables sans compromettre la facilité d'utilisation pour les employés et le personnel informatique.

Tout est compris dans le service de Cloud – il n'y a aucun matériel à installer ni de logiciels à entretenir... La MFA est désormais considérée comme une protection essentielle et elle est proposée par WatchGuard.

Tom Ruffolo
CEO, eSecurity Solutions

AUTHENTIFICATION MULTIFACTEUR

Pourquoi une authentification multifacteur est aussi importante ?

Lorsque l'on se penche sur les frais directs et indirects liés aux fuites de données, on se rend compte que l'addition peut être élevée. Lorsqu'une fuite de données survient, l'entreprise engage souvent des spécialistes afin d'en examiner les causes, prend des mesures de sécurité afin de pallier toute défaillance, peut avoir à payer des amendes réglementaires, des frais juridiques, etc. Pourtant, les frais indirects inhérents à la baisse de productivité des employés ainsi que la perte des clients présents et futurs peuvent être encore plus substantiels. Parlons chiffres... Une étude du Ponemon Institute[1] estime le **coût moyen d'une fuite de données à 141 $ par donnée compromise** pour les données sensibles..

Quelle est la probabilité que vous subissiez une fuite en raison d'un mot de passe faible ou partagé ? Les données montrent que 3 personnes sur 100[2] utilisent le mot de passe vulnérable « 123456 » et **6 personnes sur 100 utilisent le même mot de passe pour l'ensemble de leurs comptes en ligne**. Vous devez donc vous poser cette question : quelle est la probabilité qu'un ou plusieurs de vos employés aient une mauvaise gestion de leurs mots de passe ? Ceci explique sans doute pourquoi de plus en plus d'organismes de réglementation exigent une authentification à deux facteurs ou à multiples facteurs au moins pour une partie des utilisateurs des entreprises conformes – par exemple en plus de la norme de sécurité de l'industrie des cartes de paiement (PCI-DSS) v 3.2.

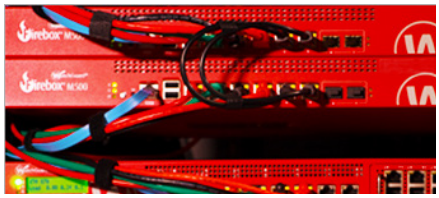
La bonne nouvelle, c'est que vous pouvez atténuer ces risques avec une authentification multifacteur basée sur le Cloud pour un prix raisonnable ! Sans devoir investir dans des infrastructures supplémentaires, des tokens physiques, et des services de support et de maintenance de logiciels, cela coûte seulement **2 € par utilisateur et par mois**, pour réduire les risques de dépenses inhérents aux fuites précédemment citées.

1 2017 Ponemon Institute Cost of Data Breach Study et 2017 Ponemon State of SMB Cybersecurity Report

2 http://fortune.com/2017/12/19/the-25-most-used-hackable-passwords-2017-star-wars-freedom/

3 https://www.statista.com/statistics/763091/us-use-of-same-online-passwords

LE PORTEFEUILLE DES SOLUTIONS DE SÉCURITÉ WATCHGUARD



Sécurité réseau

En plus de garantir une sécurité de pointe à votre entreprise, notre plateforme est spécifiquement conçue pour être facile à déployer, utiliser et gérer en continu, ce qui fait de WatchGuard la solution idéale pour les PME, les moyennes entreprises et les entreprises distribuées à travers le monde.

WiFi sécurisé

Conçue pour offrir à vos environnements WiFi un espace sûr et protégé tout en éliminant les tâches d'administration fastidieuses et en réduisant considérablement les coûts, la solution de WiFi sécurisé WatchGuard change véritablement la donne sur le marché actuel. Avec des outils d'engagement exhaustifs et une parfaite visibilité sur vos données d'entreprise, cette solution confère à votre entreprise un avantage concurrentiel.

Authentification multifacteur

WatchGuard AuthPoint™ permet de corriger cette faille de sécurité à l'aide d'une authentification multifacteur sur une plateforme Cloud simple à utiliser. L'approche unique de WatchGuard se démarque grâce au facteur « ADN de téléphone portable » qui permet de s'assurer que seules les personnes autorisées ont accès aux réseaux et aux applications Cloud sensibles.

En savoir plus

Pour plus d'informations, contactez votre revendeur agréé WatchGuard ou visitez notre site à l'adresse suivante : **https://www.watchguard.com.**.

À propos de WatchGuard

WatchGuard® Technologies, Inc. est un leader mondial de la sécurité réseau, des connexions Wi-Fi sécurisées et des produits et services de supervision réseau, et sert plus de 80 000 clients dans le monde. La société a pour mission de rendre la sécurité de pointe accessible aux entreprises de tous types et de toutes tailles, ce qui fait de WatchGuard la solution idéale pour les entreprises multisites et pour les TPE, PME, ETI et administrations. WatchGuard a établi son siège social à Seattle, aux États-Unis, et possède des bureaux dans toute l'Amérique du Nord, en Europe, en Asie-Pacifique et en Amérique latine. Pour en savoir plus, rendez-vous sur le site **WatchGuard. fr**.